(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 September 2002 (12.09.2002)

PCT

(10) International Publication Number
WO 02/071354 A2

(51) International Patent Classification[7]: G07F 19/00

(21) International Application Number: PCT/CA02/00272

(22) International Filing Date: 4 March 2002 (04.03.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/272,300 2 March 2001 (02.03.2001) US

(71) Applicant *(for all designated States except US)*: **SOFT TRACKS ENTERPRISES LTD.** [CA/CA]; Suite 1258, 13351 Commerce Parkway, Richmond, British Columbia V6V 2X7 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SWAIN, Alan, L.** [CA/CA]; 9740 Snowdon Avenue, Richmond, British Columbia V7A 2M1 (CA). **WOO, Kevin, K., M.** [CA/CA]; 10368 - 167th Street, Surrey, British Columbia V4N 1Z2 (CA).

(74) Agent: **FASKEN MARTINEAU DUMOULIN LLP**; Toronto Dominion Bank Tower, Box 20, Suite 4200, Toronto Dominion Centre, Toronto, Ontario M5K 1N6 (CA).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/071354 A2

(54) Title: SYSTEM AND METHOD FOR FACILITATING AN M-COMMERCE TRANSACTION

(57) Abstract: A method for enabling authenticated payment by a user for top-up of prepaid services through a transaction device in real-time and which use is made of existing interfaces of both the transaction device service provider and of the financial institution effecting the top-up payment, the method comprising the steps of receiving at an application server first information indicative of the transaction device authentication; receiving at the application server second information for verification of the user; and using both the first and second information to authorise top-up payment of the prepaid service.

SYSTEM AND METHOD FOR FACILITATING AN M-COMMERCE TRANSACTION

BACKGROUND OF THE INVENTION

Payments in commercial transactions have evolved over time, from cash transactions, to credit card transactions to present day payment via electronic devices. Each step in the evolution has spawned its own industry and infrastructure, and successive levels in the evolution have built on the existing infrastructure. Collectively these infrastructures and processes are referred to as the payment industry.

While wireless and Internet technologies are fuelling change within the current payment industry, there is a need for new innovative payment solutions, which leverage the hard earned trust of existing financial institutions. It is the eventual goal to effect a transformation of the payment industry by enabling secure and trusted payments, in any form of tender, via any electronic device.

In general, mobile e-commerce (m-commerce) is defined as online purchasing of goods and services, including subscription based services, such as news, music and financial services, using a mobile phone service. A major challenge inhibiting widespread adoption of m-commerce solutions today is that purchasers often do not trust a mobile device as a secure way of making online payments.

A first step in overcoming this challenge is to involve the wireless carrier as the merchant in selling its own prepaid subscription service in real time. Mobile carriers currently provide three prepay top up solutions. In the first solution, customers purchase a card such as a magnetic stripe card or similar encoding mechanism to indicate that the customer has paid a predetermined prepaid value for the card. These so-called "prepaid vouchers" are purchased at retail outlets. The code on the prepaid voucher is read by the purchaser and communicated either directly on the phone with a carrier customer service representative, or through the carrier's IVR (Interactive Voice Response) system. The code represents a monetary value, which may be added

to the balance of the customer's prepaid account maintained by the carrier. A second solution is payment via credit card, wherein credit card information is either communicated to a carrier's customer service representative via voice or through a PC based web interface. A third solution involves customers prepaying for airtime through automated telemachines (ATM's). This solution is similar to prepaid vouchers in that a code printed on the ATM receipt is communicated to the carrier's customer service representative or entered through the carrier's IVR system.

As may be seen, none of the above solutions allow immediate, secure, authenticated and non-repudiable prepay top up of the customers pre paid value via the customer's wireless telephone or similar device. Because of this, current pre-paid solutions are not as successful as anticipated.

It is thus an objective of the present invention to mitigate some of the above disadvantages.

SUMMARY OF THE INVENTION

One objective of the present invention is to enable authenticated credit transactions and real time payment for top-up of prepaid cellular phones, which uses existing interfaces at both the cell phone carrier network and at the financial institution effecting the top up payment.

In accordance with this invention there is provided a method for enabling authenticated payment by a user for top-up of prepaid services through a transaction device in real-time and which use is made of existing interfaces of both the transaction device service provider and of the financial institution effecting the top-up payment, the method comprising the steps of receiving at an application server first information indicative of the transaction device authentication; receiving at the application server second information for verification of the user; and using both the first and second information to authorize top-up payment of the prepaid service

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the preferred embodiments of the invention will become more apparent in the following detailed description in which reference is made to the appended drawings wherein:

Figure 1 is schematic diagram of a payment system according to the present invention;

Figure 2 is a schematic diagram of a payment system according to one embodiment of the invention;

Figure 3 is a schematic diagram of a payment system according to another embodiment of the invention;

Figures 4, 5, 6 and 7 show ladder diagrams for use-case scenarios of the system of figure 3.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In the following description like numerals refer to like structures in the drawings. For convenience, the definitions, acronyms, and abbreviations used in the description are listed in table 1

Table I

Acronym/ Abbreviation	Expansion
TGS	Transaction Gateway Server
AS	Application Server
RTP	Real Time Payment
MWS	Merchant Wallet Server
VTS	Virtual Terminal Server
IVR	Interactive Voice Response
MT	Mobile Terminal
CDPD	Cellular Digital Packet Data

Acronym/ Abbreviation	Expansion
ASCII	American Standard Code for Information Interchange

Referring now to Figure 1, there is shown a block diagram of the main components in a system 100 for facilitating prepaid-type transactions according to an embodiment of the present invention. This system includes an application server (AS) 120 for processing transaction requests from at least one wireless device 122, such as a cellular telephone, the application server 120 is also capable of forwarding transactions to an acquiring financial institution 124a or an issuing financial institution depending on whether the transaction is, respectively, a credit card transaction or a real time payment (RTP) transaction. A real time payment transaction refers to a payment mechanism where funds from the purchaser's bank account are debited in near real time. The system 100 also includes a merchant wallet server (MWS) 126, which acts as a proxy between a Virtual Terminal Server (VTS) and one or more electronic wallets (e-Wallets) 130 containing user credit card numbers, bank ATM card numbers or bank account numbers, stored value account numbers, billing addresses and shipping addresses stored in a carrier subscriber database 132. The MWS is able to extract information from the e-wallets130 and present them in a form that can be used by the VTS. In effect, the MWS acts as a front end to the VTS, enabling the support of m-commerce.

Credit card and RTP transactions may also be sent through a transaction gateway server (TGS) 134 to the acquiring bank's 124a interface.

The system 100 may also include carrier's IVR server 136, which transmits payment information to the AS. Payment information captured by a carrier's IVR system is sent to the AS in the same manner as that of a WAP enabled phone. Information entered by the IVR system is combined with information stored at the carrier's subscriber database. Credit card and RTP transactions are then routed to a TGS. The

TGS is an optional intermediary in communication with the various financial institutions.

The prepaid transactions of the present invention are facilitated by payment applications (PA) running on the AS. The AS is a multi-application server, which allows for a variety of different payment methods and tender types. The payment applications have support for tender types such as credit card, cash, cheque, and e-Wallets. The e-Wallets themselves may contain references to credit cards, bank accounts, and stored value accounts. In addition, the payment application has an Enterprise Reporting feature allowing reports on usage per subscriber. An important feature of the AS is the ability to route the prepay transactions to the appropriate processing interface based on the payment type. In the case of WAP enabled digital phones, the owner of the prepaid mobile device communicates with the AS via the payment application residing on the AS. Information entered by the user, along with information kept within the carrier's prepaid database / e-Wallet is aggregated in the AS. The AS handles payment types as described below.

The payment types supported by the system 100 are generally credit card transactions and RTP transactions. With each of these payment types, there are different levels of device 122 and user authentication, different interface requirements, and differences in response mechanisms. The transaction types implemented will require mutual resolution and agreement between the parties.

Non-Face-To-Face Transactions Using Credit Cards

In a credit card transaction, only the credit card number of the prepaid user is stored in a subscriber e-Wallet 130. This is what is currently used to effect Internet based payment. There is no authentication for the card or account, no authentication of the owner of the card or account and no authentication of the owner's intent to complete the transaction as is evidenced in a card present credit card transaction when the card is swiped and the owner signs the receipt or as is evidenced in an on-line debit transaction when the card is swiped and the owner of a debit card enters a secret PIN

associated with the debit card. Rather, this type of transaction is typically called a Mail Order Telephone Order (MOTO) transaction. This does not fulfill general requirements of a go-to-market strategy for m-Commerce as these types of transactions can be easily repudiated and hence are highly subject to fraud. This invention enables m-commerce transactions that can generally not be repudiated. This invention meets the general requirements for non-repudiation of ensuring that the transaction process itself requires something that only the consumer has in possession and that the consumer intended to complete the transaction by requiring consumer to securely disclose to the system, something that only the consumer knows. The challenge of m-Commerce to achieve this is made even more difficult as often, the consumer and the merchant are not face-to-face as is the case with a an on-line credit card or an on-line debit card transaction.

Credit Card with Subscriber Device Authentication

Subscriber handset identities (SID) are commonly used within cellular networks to authenticate user phones. In this case, a credit card number is associated with the phone's secure identity to satisfy the concept of a virtual card. Currently, to effect a card present transaction, the card must be physically swiped and the data (called track2 data) on the magstripe of the card must be captured. If a trust relationship is set up between the carrier and the financial institution, the combination of the phone's secure identity and credit card number represents an equivalent risk to a card present transaction. This may be referred to as a "virtual card present transaction".

Credit Card with Subscriber Device & Password Authentication

Building on the virtual credit card transaction, a password can be associated with the subscriber's e-Wallet. The password is used to authenticate the owner of the e-Wallet (i.e. the subscriber), allowing access to the associated virtual credit card contained in the e-Wallet. User authentication lowers the risk of fraud involved in using a virtual credit card. By agreement between the owner of the e-Wallet and the e-Wallet service provider, the use of a password to authenticate the subscriber can be considered as a replacement for a signed receipt for purposes of non-repudiation.

RTP through EFT

The AS can route RTP transactions via the TGS to an Electronic Funds Transfer (EFT) interface of banks. This mechanism transfers money from the subscriber's bank account to the merchant's bank account overnight. The attractiveness of EFT is the ability to handle transactions for all banks through one interface. The EFT backend deals with the transfer of funds between the individual banks. A limitation of the EFT interface is that payment transfers are typically delayed up to 24 hours, and are not immediate. Responses are typically batched into one file and extracted from the EFT interface, when the file is available. Therefore, prepay top up transactions may take up to 24 hours before receiving a response from the bank, hence failing to meet a real time acknowledgement requirement.

This delay is addressed in one of several ways. A first option is that the financial institution processes and acknowledges an EFT transaction in real time in a scenario where the merchant (i.e. carrier) account and subscriber account is within its own domain. A second option is that a notification is sent to the subscriber some time in advance when the number of minutes still remaining in the subscriber's prepay account is below a certain level so that the 24-hour delay is inconsequential.

RTP through Real Time Payment Gateway

The AS can route RTP transactions via the TGS to evolving bank interfaces. The goal of these interfaces is to process funds transfer transactions in real time. Transactions belonging to the bank, hosting the interface, may be processed in real time. These interfaces, often based on XML standards such as OFX, provide a real time confirmation for a given transaction, unlike an EFT interface. Real time responses allow a subscriber to issue a payment transaction online and wait for the acknowledgement. Within this scenario the financial institution can only process and acknowledge transactions in real time when the subscriber holds an account at that bank.

Debit Transactions

With Debit transactions networks such as the Interac™ network the underlying principles of authentication can be satisfied with today's cellular security and

authentication technologies, hence making debit transactions acceptable, most especially in the closed environment of prepay.

As described earlier, the MWS acts as a proxy between the VTS and e-Wallets that hold subscriber credentials. The MWS combines information from e-Wallets and information entered from either the carrier's IVR system or the WAP based prepay application. The information is used to construct a credit or RTP transaction. Once a successful response message is received, the MWS is responsible for notifying both the user of the mobile device, and the carrier's prepay subscriber database. The response can be sent to the WAP based prepay application or the carrier's IVR system. In the case that the subscriber database held at the carrier receives a successful response, the appropriate amount is added to the user's prepaid account.

Another feature of the MWS is the ability for a merchant to be authenticated as part of the transaction. Merchant credentials can be securely stored within the MWS and can be included in the transaction details, if the bank requires. This is a major step towards having the ability to authenticate both the subscriber and the merchant in a financial transaction. Optionally, if a PKI-enabled MWS is used, merchant credentials can be encrypted and digitally signed before sending the authentication to the bank. There are three e-Wallet configurations that the MWS supports.

Bank Hosted Wallet Server 140

The bank may choose to hold all of the subscriber's credentials within their own e-Wallet. The carrier's subscriber database is used as an authentication mechanism to enable payment through the bank e-Wallet. One authentication scheme involves the use of a token, which is stored at the subscriber database held at the carrier, and that token is used to extract subscriber credentials within the bank e-Wallet. This token can take the form of a PKI public key or certificate. If the prepay user has multiple e-Wallets with different banks, the carrier's subscriber database facilitates an authentication mechanism for each of the e-Wallets.

Carrier Hosted Wallet Server 130

The MWS can operate in an environment where a carrier hosts an e-Wallet. User information, along with credit card numbers and bank account numbers is held within the carrier's e-Wallet. This information is sent to the MWS, when a prepay top up transaction is being constructed. There is also a method for the MWS to update the user prepay account information at the carrier's subscriber database. In this scenario, the carrier subscriber database is proxied by the e-Wallet server. Therefore, once a response from a top up transaction is received, the MWS passes the details of the response to the e-Wallet server. The e-Wallet server, in turn, updates the users prepay account information held within the subscriber database.

Carrier and Bank Jointly Hosts the Wallet Server

The bank may choose to hold some of the e-Wallet credentials such as bank account information. They may also choose to hold only those credentials pertaining to the particular bank. This is an example of a multiple e-Wallet implementation. The MWS is capable of supporting connections to multiple e-Wallet servers whether they are hosted at the carrier or the bank.

While the overall system components, and payment types handle by the system have been describe above, the security mechanism implemented by the system 100 is now described.

Device Authentication

A device can be authenticated before any interactions with a financial institution. Carriers use subscriber identity authentication mechanisms and other security measures to safeguard the security and identity of a cellular phone. This technology, especially in the digital space has proven effective in authentication of mobile phones. The MWS solution builds on the carrier's authentication mechanisms. A devices authenticated identity is associated with a credit card number creating the notion of a virtual credit card. In actuality, the carrier's authentication procedure will enable the first step in granting access to a subscriber's e-Wallet that contains a subscriber's virtual credit cards. A password is used to authenticate the owner of the e-Wallet and

forms the second step in granting access to transact with the virtual credit cards in the e-Wallet.

User Authentication

To enable a prepay transaction, the carrier may choose to authenticate the user before accepting the transaction. There may be one or more passwords depending on the payment method. Typically, an e-Wallet password will be required to initiate a top up transaction. A second password may be needed to affect an RTP transaction. This is similar to an online bill payment scenario, where typically a username and password is required. The subscriber handset identity (SID) is used in place of the username. By agreement between the owner of the e-Wallet and the e-Wallet service provider, the use of a password to authenticate the subscriber can be considered as a replacement for a signed receipt for purposes of non-repudiation. PKI technologies will be implemented as these technologies mature within cellular devices.

Communication between Infrastructure Components

Standard Secure Sockets Layer (SSL) communications protocols are implemented on wide-area communications.

Referring to figure 2, there is shown another embodiment of the system 200 of the present invention. The system 200 comprises four interfaces into the AS, namely a carrier IVR system, carrier WAP gateway, carrier subscriber database via the e-Wallet, and the financial institution's acquiring interface via the TGS. It is noted that the carrier subscriber database is represented as an entity that accepts transaction responses and exception codes.

This implementation builds on the existing carrier infrastructure and requires only changes to the carrier's IVR system interface so that the IVR system communicates with the AS. All other four interfaces stay intact.

Prepay top up transactions can originate from either the carrier's IVR system or a WAP enabled phone. The IVR system communicates via an IP based connection into the AS business logic. XML based communications protocols may be used.

Whereas, the WAP enabled phone will access a prepay application hosted at the AS. Although, both mechanisms use different input strategies, the backend processing does not change.

The e-Wallet function has been split up into two components. The first component is an implementation of a simple e-Wallet for storage of subscriber payment information. The second component is the subscriber database that is currently in use at the carriers. When a top up transaction is created, user credentials are retrieved from the e-Wallet. This information is combined with the information entered by the user to affect the transaction. Once a transaction response has been received, an account update request is sent from the MWS to the subscriber database via the e-Wallet server. Both types of payment types are supported: credit card, and RTP.

Referring to figure 3, there is shown a further embodiment of an implementation of the system 100. In this scenario, the subscriber prepay database function has been separated from the client e-Wallet server. Once a transaction response has been received, an account update request is sent from the MWS directly to the subscriber database. Transaction details may be sent to the e-Wallet server to provide the subscriber with a transaction history.

Referring to figure 4, there is shown a ladder diagram describing a first use case for the embodiment of figure 3. This use-case describes a subscriber initiated prepay via WAP Phone scenario.

This scenario is a two-step transaction. The subscriber is involved in two phone sessions, where the second session is used as a further subscriber authentication step. The first session involves the subscriber affecting a prepay application. The prepay application may be accessible from either the WAP browser's default menu or by typing the URL of the application. The second session involves pushing an alert back to the subscriber. The second step removes the possibility that the original prepay transaction was not initiated by the intended subscriber. The subscriber ID of the

mobile device held within the e-Wallet defines the destination device of the push alert.

Each of the steps in the ladder diagram of figure 4 may be described as follows:

1. The subscriber enters the URL of WAP prepay application.
2. The carrier network validations ESN and MIN of subscriber phone.
3. Secure session is initiated with WAP gateway and prepay application host – the subscriber ID (SID) of the phone is passed to the application in the request header.
4. The subscriber is prompted by the prepay application for additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.
5. Prepay application builds an XML based message and sends the message to the MWS. The request will minimally contain the SID for device authentication and optionally a password for subscriber authentication.
6. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.
7. Based on the SID, the subscriber's credentials are extracted from the e-Wallet. Optionally, if a password has been specified, the SID and password pair is authenticated against the SID and password held in the e-Wallet.
8. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.
9. An XML based response message is sent back to the prepay application. The transaction ID assigned to the temporary prepay

transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the SID extracted from the e-Wallet is sent to enable the WAP push mechanism in the next step.

10. The web server generates a WAP push message out to the subscriber device. The destination device can be determined by the SID. The push message can take the form of a real WAP push message through the WAP browser, or an indirect WAP push through the SMS messaging mechanism of the phone. In either case, the push message will contain a URL for triggering the prepay transaction. To complete the authentication loop, the URL will consist partly of the transaction ID of the temporary prepay transaction held at the MWS.

11. The subscriber authorizes the prepay transaction by selecting the URL and confirming the transaction.

12. The prepay web server sends a second XML based request to the MWS, which is an authorization request (confirmation) of the original prepay transaction.

13. The MWS sends the payment request to the VTS using an XML based protocol.

14. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.

15. The TGS processes the transaction through the financial payment gateway.

16. The TGS receives a transaction response from the financial payment gateway.

17. The transaction response is routed back from the TGS to the VTS.

18. The transaction result is passed from the VTS to the MWS.

19. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the subscriber device. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.

20. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may optionally be viewable from the online customer care website as a prepay transaction history.

21. To update the subscriber's device, the prepay result is sent from the MWS to the payment application.

22. The payment application generates a WAP push on the subscriber's device notifying the subscriber the prepay transaction has been processed.

Referring to figure 5, there is shown a ladder diagram describing a second use case for the embodiment of figure 3. This use case describes a System Initiated Prepay Via WAP Phone scenario.

This scenario is a one-step transaction. Unlike the subscriber initiated prepay, described with reference to figure 4, we are certain that the push alert will arrive at the intended subscriber device. A process continuously monitors the prepay database. If a subscriber's prepay amount falls below a certain threshold, a push alert is generated from the system. The subscriber acts on this push alert to affect a prepay transaction.

Each of the steps in the ladder diagram of figure 5 may be described as follows:

1. A database trigger is setup within the prepaid database. Once a subscriber's prepay amount falls below a certain threshold, an event is

generated and a request is made to the MWS to initiate a prepay transaction. The request will also contain a reference to the subscriber record within the e-Wallet.

2. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.

3. The subscriber's credentials are extracted from the e-Wallet. Since the system is initiating a prepay request, the password held at the e-Wallet does not need to be validated.

4. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.

5. An XML based response message is sent back to the prepay application. The transaction ID assigned to the temporary prepay transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the SID extracted from the e-Wallet is sent to enable the WAP push mechanism in the next step.

6. The web server generates a WAP push message out to the subscriber device. The destination device can be determined by the SID. The push message can take the form of a real WAP push message through the WAP browser, or an indirect WAP push through the SMS messaging mechanism of the phone. In either case, the push message will contain a URL for triggering the prepay transaction. To complete the authentication loop, the URL will consist partly of the transaction ID of the temporary prepay transaction held at the MWS.

7. The subscriber authorizes the prepay transaction by selecting the URL and confirming the transaction. The subscriber is also prompted for

additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.

8. The prepay web server sends an XML based request to the MWS, which is an authorization (confirmation) of the prepay transaction.
9. The MWS sends the payment request to the VTS using an XML based protocol.
10. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.
11. The TGS processes the transaction through the financial payment gateway.
12. The TGS receives a transaction response from the financial payment gateway.
13. The transaction response is routed back from the TGS to the VTS.
14. The transaction result is passed from the VTS to the MWS.
15. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the subscriber device. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.
16. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may optionally be viewable from the online customer care website as a prepay transaction history.
17. To update the subscriber's device, the prepay result is sent from the MWS to the payment application.

18. The payment application generates a WAP push on the subscriber's device notifying the subscriber the prepay transaction has been processed.

Referring to figure 6, there is shown a ladder diagram describing a third use case for the embodiment of figure 3. This use case describes a Subscriber Initiated Prepay Via IVR System scenario.

This scenario is a two-step transaction. The subscriber is involved in two IVR sessions, where the second session is used as a further subscriber authentication step. The first session involves the subscriber affecting a prepay application. The second session involves pushing an alert back to the subscriber. The push alert takes the form of a phone call to the subscriber device. The second step removes the possibility that the original prepay transaction was not initiated by the intended subscriber. The phone number (Mobile Identity Number, MIN) held within the e-Wallet defines the destination device of the push alert.

Each of the steps in the ladder diagram of figure 6 may be described as follows:

1. The subscriber dials the IVR system through the subscriber's device. The prepay application is selected from the list of options.
2. The carriers network validations ESN and MIN of subscriber phone.
3. The subscriber is prompted by the IVR system for additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.
4. The IVR system builds the appropriate XML based message and sends the message to the MWS. The request will minimally contain the MIN for device authentication and optionally a DTMF password for subscriber authentication. The assumption is that caller ID is activated for the subscriber's device; therefore, the IVR system receives and passes through the MIN of the phone.

5. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.

6. Based on the MIN, the subscriber's credentials are extracted from the e-Wallet. Optionally, if a password has been specified, the SID and password pair is authenticated against the SID and password held in the e-Wallet.

7. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.

8. An XML based response message is sent back to the IVR system. The transaction ID assigned to the temporary prepay transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the MIN extracted from the e-Wallet is sent to enable the IVR callback in the next.

9. An IVR callback to the subscriber phone is performed using the MIN sent from the MWS. The IVR system outlines the transaction details to the subscriber. To complete the authentication loop, the IVR system will temporarily hold the transaction ID of the temporary prepay transaction held at the MWS.

10. The subscriber authorizes the prepay transaction through the IVR system.

11. The IVR system sends a second XML based request to the MWS, which is an authorization (confirmation) request of the original prepay transaction.

12. The MWS sends the payment request to the VTS using an XML based protocol.

13. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.

14. The TGS processes the transaction through the financial payment gateway.

15. The TGS receives a transaction response from the financial payment gateway.

16. The transaction response is routed back from the TGS to the VTS.

17. The transaction result is passed from the VTS to the MWS.

18. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the IVR system. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.

19. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may optionally be viewable from the online customer care website as a prepay transaction history.

20. To update the subscriber device, the prepay result is sent from the MWS to the IVR system.

21. The IVR system calls the subscriber's device notifying the subscriber the prepay transaction has been processed.

Referring to figure 7, there is shown a ladder diagram describing a third use case for the embodiment of figure 3. This use case describes a System Initiated Prepay Via IVR System scenario.

This scenario is a one-step transaction. Unlike the subscriber initiated prepay, we are certain that the IVR callback mechanism will arrive at the intended subscriber device. A process continuously monitors the prepay database. If a subscriber's prepay amount falls below a certain threshold, an IVR phone call is generated from the system. The subscriber confirms through the IVR system to affect a prepay transaction.

Each of the steps in the ladder diagram of figure 7 may be described as follows:

1. A database trigger is setup within the prepaid database. Once a subscriber's prepay amount falls below a certain threshold, an event is generated and a request is made to the MWS to initiate a prepay transaction. The request will also contain a reference to the subscriber record within the e-Wallet.

2. The MWS has the possibility of connecting to one or more e-Wallets based on the carrier. A mapping between carriers and e-Wallet servers is maintained within the MWS. A request is made from the MWS to the appropriate e-Wallet server.

3. The subscriber's credentials are extracted from the e-Wallet. Since the system is initiating a prepay request, the password held at the e-Wallet does not need to be validated.

4. Once the MWS has received the subscriber's credentials, the prepay transaction is built and stored temporarily. The status of this prepay transaction is set to pending, awaiting confirmation of the transaction. A unique transaction ID for the prepay transaction is generated.

5. An XML based response message is sent back to the prepay application. The transaction ID assigned to the temporary prepay transaction is sent within the XML based message – this transaction ID is needed to confirm the prepay transaction. Additionally, the MIN extracted from the e-Wallet is sent to enable the IVR callback mechanism in the next step.

6. The IVR system outlines the transaction details to the subscriber. To complete the authentication loop, the IVR system will temporarily hold the transaction ID of the temporary prepay transaction held at the MWS.

7. The subscriber authorizes the prepay transaction through the IVR system. The subscriber is also prompted for additional field information to complete the transaction. Fields may include prepay amount, credit card or real-time payment (RTP) information.

8. The prepay web server sends an XML based request to the MWS, which is an authorization (confirmation) of the prepay transaction.

9. The MWS sends the payment request to the VTS using an XML based protocol.

10. The payment transaction request is routed from the VTS to the appropriate TGS depending on the merchant to financial institution configuration.

11. The TGS processes the transaction through the financial payment gateway.

12. The TGS receives a transaction response from the financial payment gateway.

13. The transaction response is routed back from the TGS to the VTS.

14. The transaction result is passed from the VTS to the MWS.

15. The MWS is responsible for prepay update request to the carrier's prepay database, and response messages to the e-Wallet server and the IVR system. The MWS sends a request to the prepay database to update the subscriber's prepay account with the appropriate number of minutes. It is assumed that the change in the prepay database will be reflected in the online customer care website.

16. For the purposes of tracking, the transaction details are also sent to the e-Wallet for data warehousing. These transaction details may

optionally be viewable from the online customer care website as a prepay transaction history.

17. To update the subscriber device, the prepay result is sent from the MWS to the IVR system.

18. The IVR system calls the subscriber's device notifying the subscriber the prepay transaction has been processed.

Accordingly it may be seen that the system of the present invention provides a secure real-time top-up service that can be implemented in existing payment infrastructures.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method for enabling authenticated payment by a user for top-up of prepaid services through a transaction device in real-time and which use is made of existing interfaces of both the transaction device service provider and of the financial institution effecting the top-up payment, said method comprising the steps of:

(a) receiving at an application server first information indicative of the transaction device authentication;

(b) receiving at said application server second information for verification of said user; and

(c) using both said first and second information to authorize top-up payment of said prepaid service from said financial institution.

2. A method as defined in claim 1, said prepaid service being a prepaid cellular phone.

3. A method as defined in claim 2, said first information being a hardware identification of said cellular telephone.

4. A method as defined in claim 2, said second information being a personal identification number (PIN) of said user.

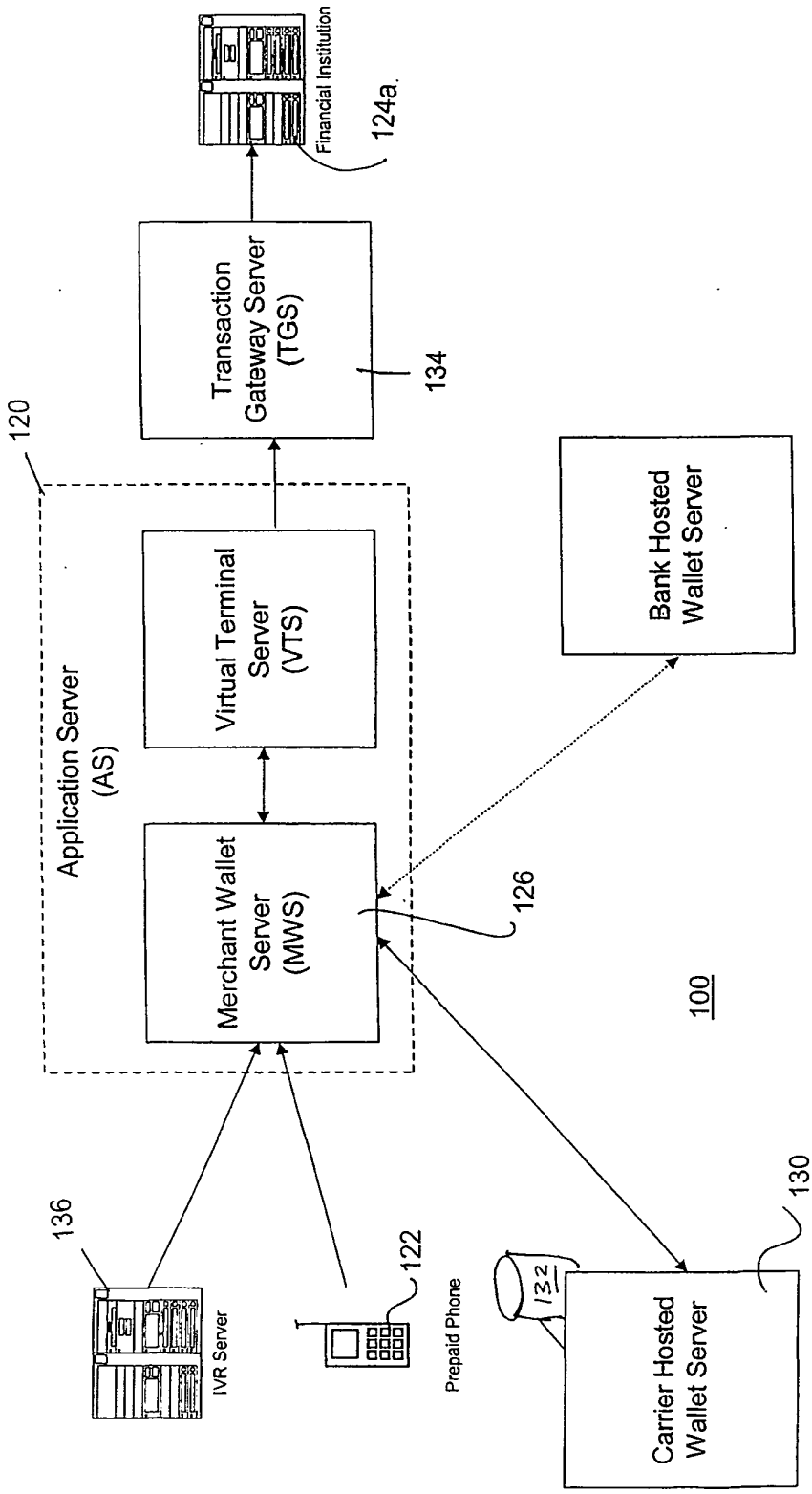
Financial Institution
124a
Transaction Gateway Server (TGS)
134
120
Application Server (AS)
Virtual Terminal Server (VTS)
Merchant Wallet Server (MWS)
126
Bank Hosted Wallet Server
100
136
IVR Server
122
Prepaid Phone
132
130
Carrier Hosted Wallet Server

Figure 1

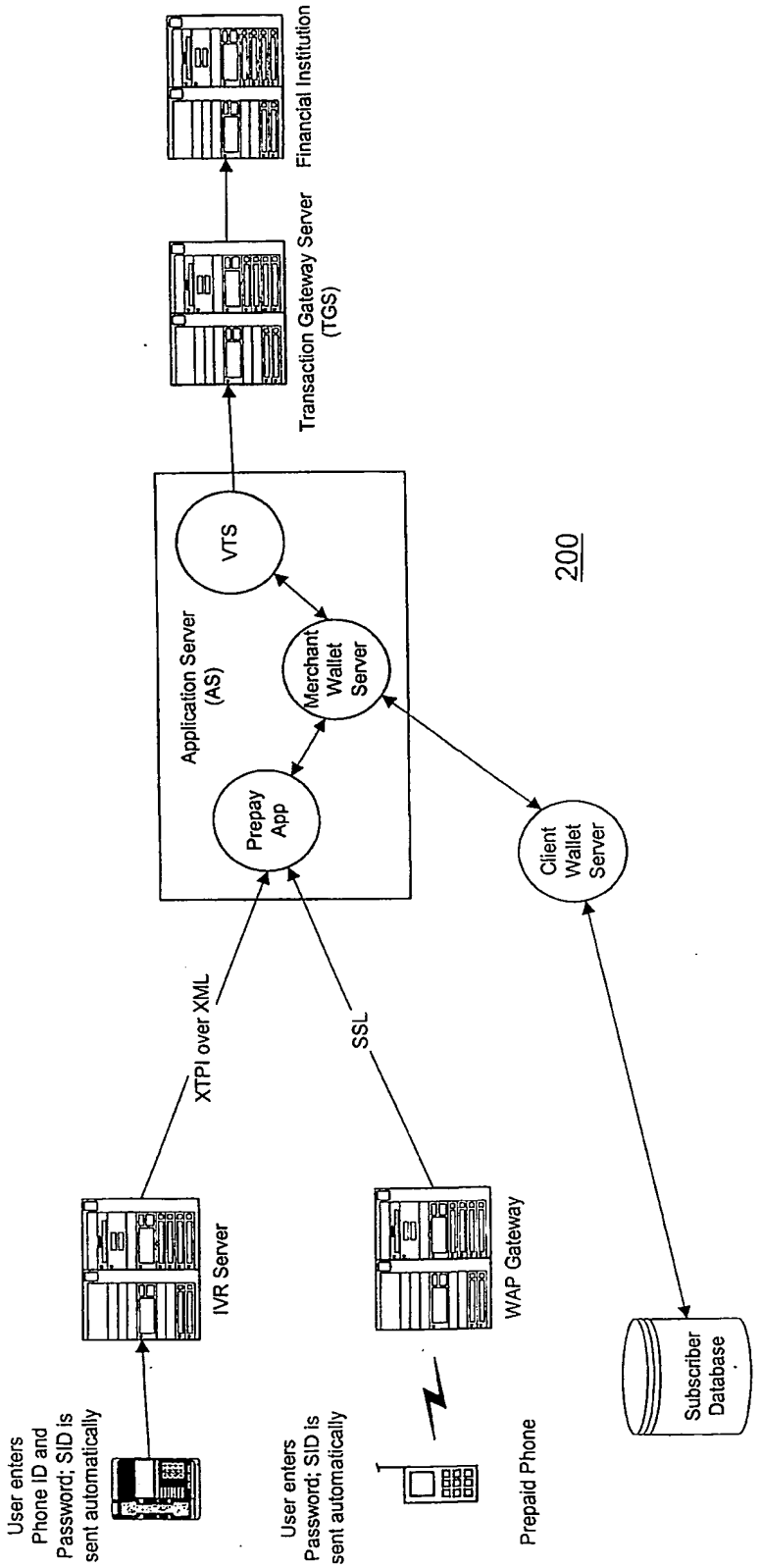
Financial Institution
Transaction Gateway Server (TGS)
VTS
Application Server (AS)
Merchant Wallet Server
Prepay App
Client Wallet Server
200
XTPI over XML
SSL
IVR Server
WAP Gateway
Subscriber Database
User enters Phone ID and Password; SID is sent automatically
User enters Password; SID is sent automatically
Prepaid Phone

Figure 2

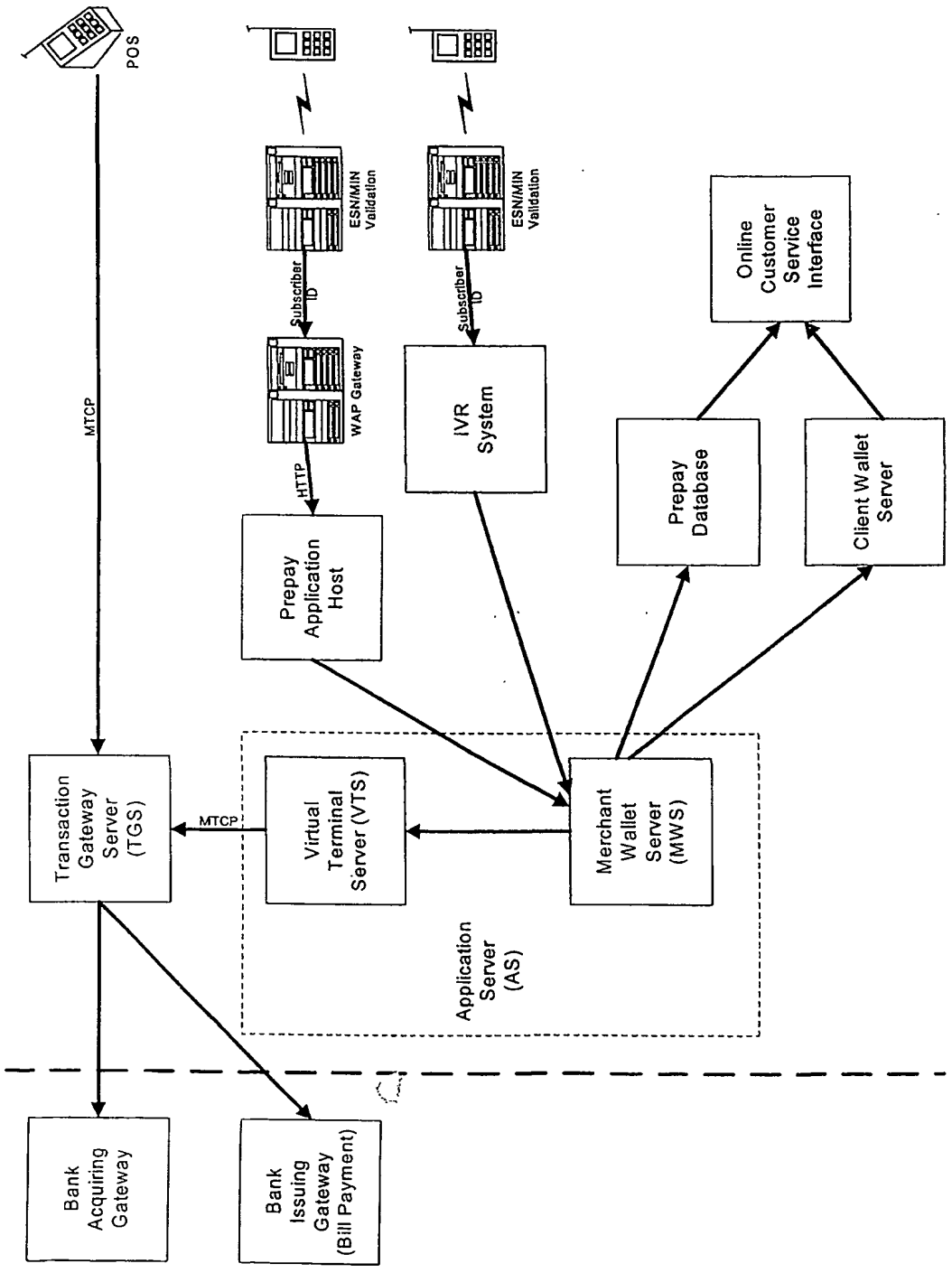
POS
MTCP
ESN/MIN Validation
ESN/MIN Validation
Subscriber ID
Subscriber ID
WAP Gateway
HTTP
IVR System
Online Customer Service Interface
Prepay Application Host
Prepay Database
Client Wallet Server
Transaction Gateway Server (TGS)
MTCP
Virtual Terminal Server (VTS)
Merchant Wallet Server (MWS)
Application Server (AS)
Bank Acquiring Gateway
Bank Issuing Gateway (Bill Payment)

Figure 3

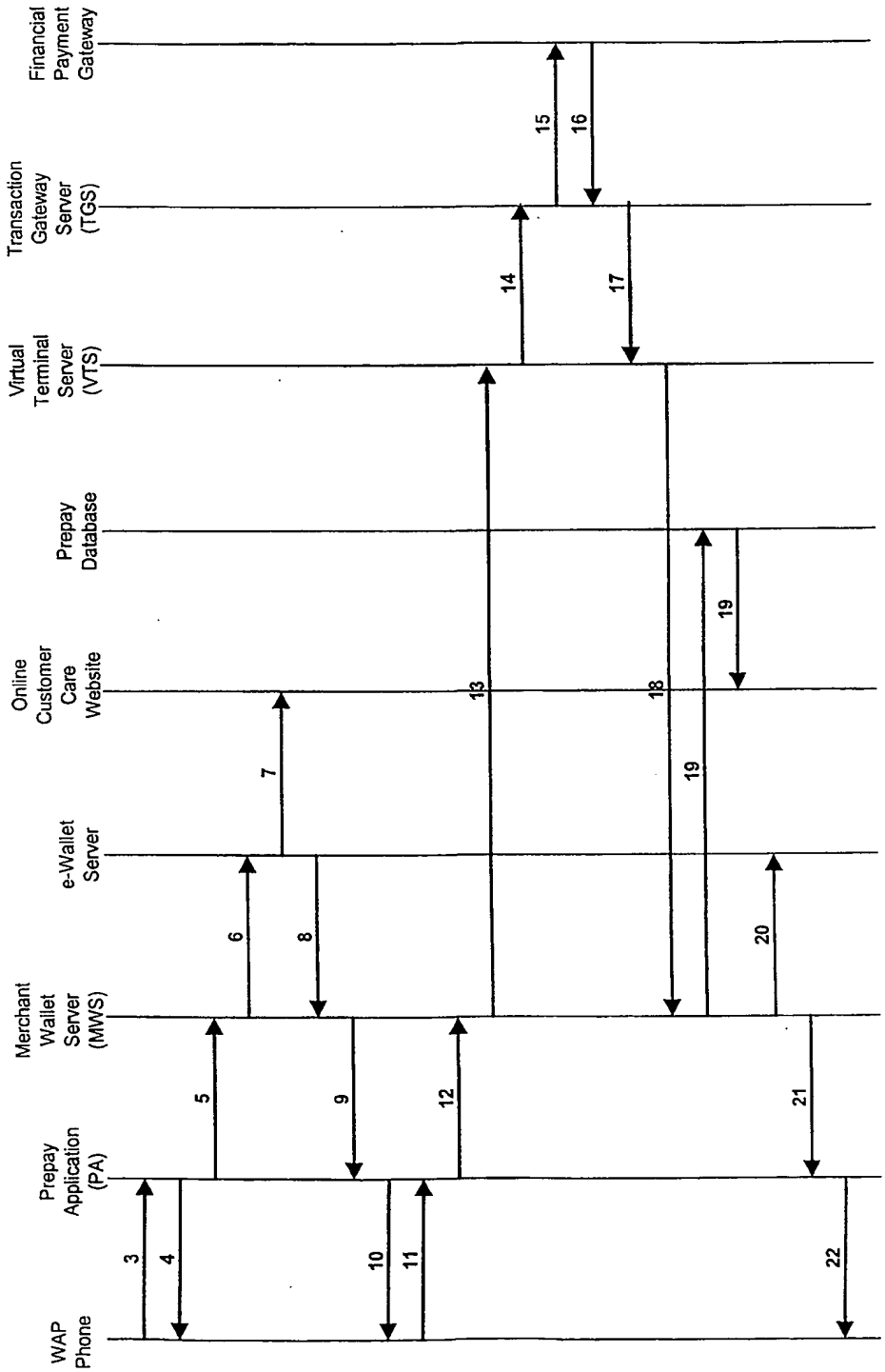
Financial Payment Gateway
Transaction Gateway Server (TGS)
Virtual Terminal Server (VTS)
Prepay Database
Online Customer Care Website
e-Wallet Server
Merchant Wallet Server (MWS)
Prepay Application (PA)
WAP Phone
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

Figure 4

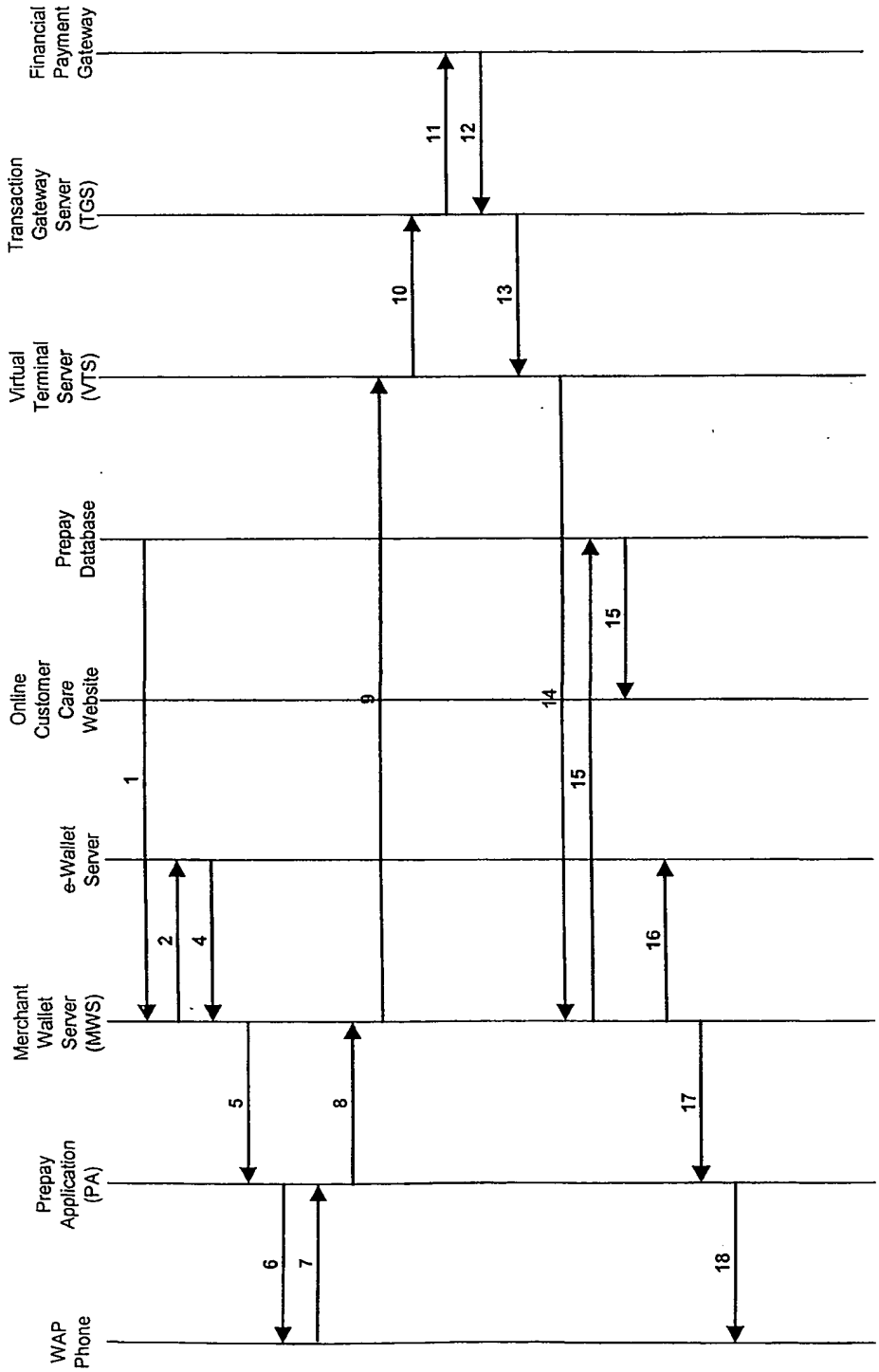
Financial Payment Gateway
Transaction Gateway Server (TGS)
Virtual Terminal Server (VTS)
Prepay Database
Online Customer Care Website
e-Wallet Server
Merchant Wallet Server (MWS)
Prepay Application (PA)
WAP Phone
1
2
4
5
6
7
8
9
10
11
12
13
14
15
15
16
17
18

Figure 5

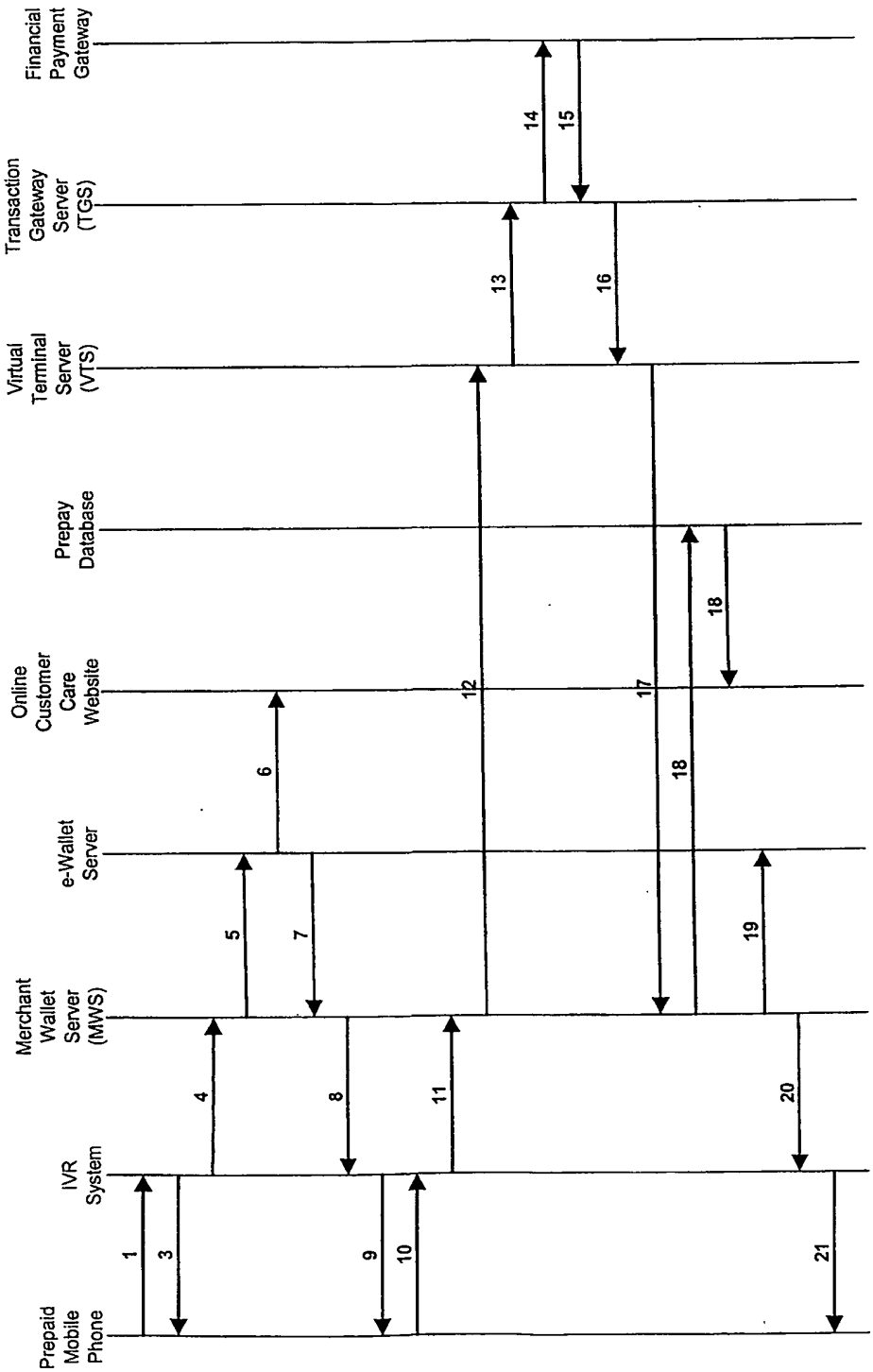
Financial Payment Gateway
Transaction Gateway Server (TGS)
Virtual Terminal Server (VTS)
Prepay Database
Online Customer Care Website
e-Wallet Server
Merchant Wallet Server (MWS)
IVR System
Prepaid Mobile Phone
1
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

Figure 6

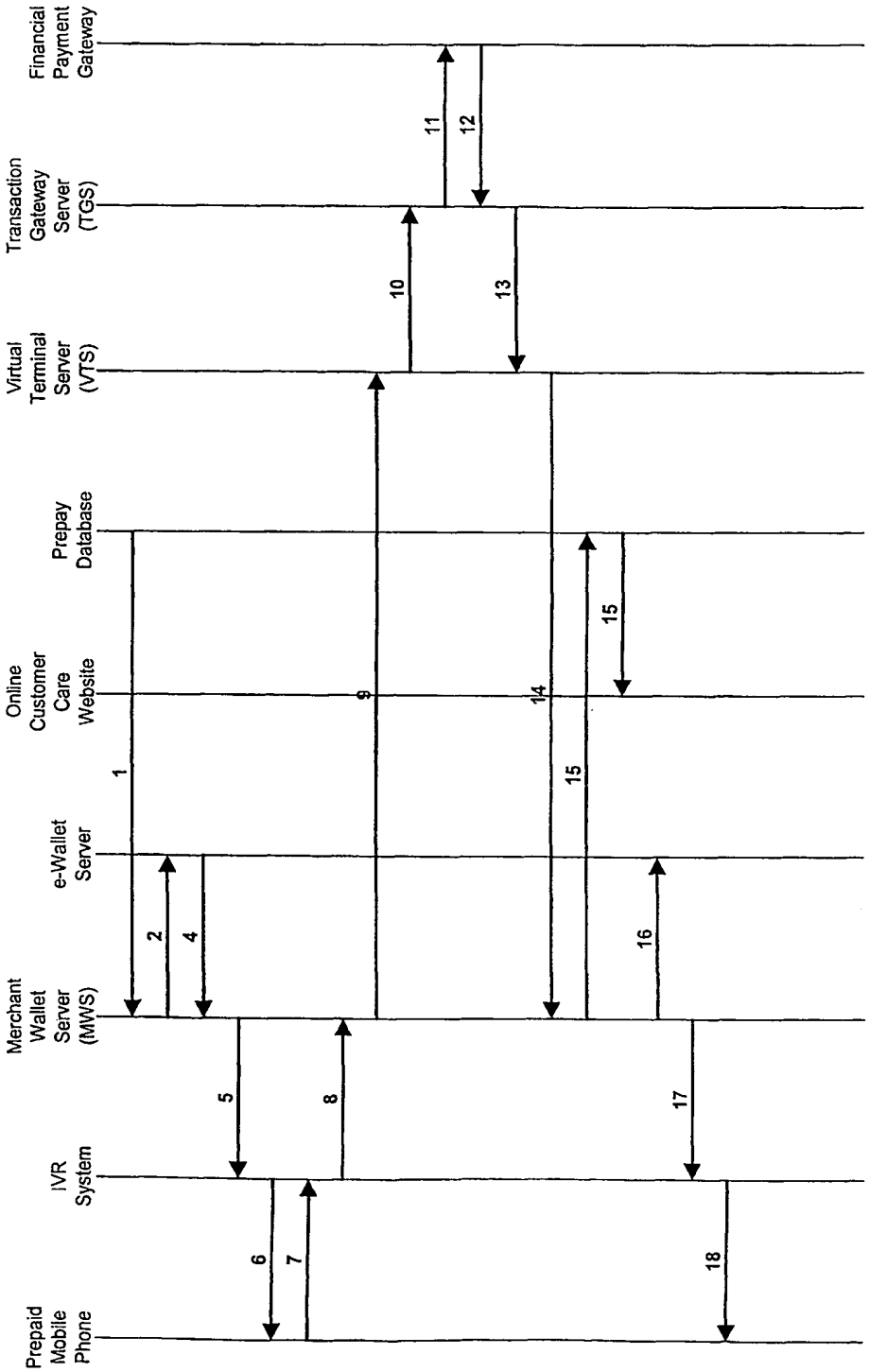
Financial Payment Gateway
Transaction Gateway Server (TGS)
Virtual Terminal Server (VTS)
Prepay Database
Online Customer Care Website
e-Wallet Server
Merchant Wallet Server (MWS)
IVR System
Prepaid Mobile Phone
1
2
4
5
6
7
8
9
10
11
12
13
14
15
15
16
17
18

Figure 7